

REMARKS/ARGUMENTS

In the Official Action mailed **13 January 2006** the Examiner reviewed claims 1-10, 13-22, and 25-33. Claims 1-5, 9, 13-17, 21, and 25-29 were rejected under 35 U.S.C. §103(a) as being unpatentable over Devarakonda et al. (USPN 6,424,992, hereinafter “Devarakonda”) in view of Kunzelman et al. (USPN 6,041,357, hereinafter “Kunzelman”) in further view of Davis et al. (USPN 6,367,009, hereinafter “Davis”) in further view of Haller et al. (USPN 6,363,363 hereinafter “Haller”) and in further view of Davis et al. (USPN 6,282,522 hereinafter “Davis, V”). Claims 6, 7, 10, 18, 19, 22, 30, 31, and 33 were rejected under 35 U.S.C. §103(a) as being unpatentable over Devarakonda, Kunzelman, Davis, Haller and Davis, V, and further in view of Fielder et al. (USPN 6,105,133, hereinafter “Fielder”). Claims 8, 20, and 32 were rejected under 35 U.S.C. §103(a) as being unpatentable over Devarakonda, Kunzelman, Davis, Haller and Davis, V, and in further view of Kennedy et al. (USPN 6,134,582, hereinafter “Kennedy”).

Rejections under 35 U.S.C. §103(a)

Independent claims 1, 13, and 25 were rejected as being unpatentable over Devarakonda, Kunzelman, Davis, Haller, and Davis, V.

Applicant respectfully points out that Devarakonda and Kunzelman *teach away* from the present invention.

Devarakonda is directed towards routing an SSL communication request from a client “*to the same [server] node*” that processed previous SSL communication requests from the client (Devarakonda, col. 4, line 66 through col. 5, line 5). Communication between a client and a sever node can reuse a session key during the session key’s lifetime (Devarakonda, col. 3, lines 43-44). However, if an SSL request from the client is routed to another server node, it

would require “*re-negotiating a [new] session key, which is an expensive operation*” (Devarakonda, col. 3, lines 44-48, col. 5, lines 24-27). The invention of Devarakonda prevents this expensive operation by routing SSL connection requests from a client “*to the same [server] node*” (Devarakonda, col. 4, line 66 through col. 5, line 5).

In contrast, the present invention facilitates routing of an SSL connection request from a client **to a different server node** without requiring key re-negotiation. In prior art techniques, “*a client must set up and maintain a separate SSL connection [with] each server [node], which can greatly degrade the scalability of the system*” (page 3, lines 1-2). For example, in the invention of Devarakonda, if an SSL request from the client is routed to a different server node, it requires “*re-negotiating a [new] session key, which is an expensive operation*” (Devarakonda, col. 3, lines 44-48, col. 5, lines 24-27). The present invention solves this key re-negotiation problem by providing “*a system for sharing [an SSL] session with a client between a plurality of servers*” (page 3, lines 25-26). The system can share an SSL session between servers by performing the steps shown in FIGs. 5 & 6 of the instant application. Specifically, a first server retrieves “*security state information from [the] second server, which has an active secure communication session with the client*” (page 4, lines 5-6, FIG. 5, 506, 508). The first server then “*uses this state information to establish the active secure communication session with the client*” (page 4, lines 7-9, FIG. 5, 510). Next, the second server “*purges state information from its local store so that another server does not request and receive the same state information*” (page 14, lines 8-10, FIG. 6, 612). To summarize, Devarakonda teaches away from the present invention, because, in contrast to Devarakonda, the present invention does not require re-negotiating a new session key when an SSL request from the client is routed to a different server node.

Kunzelman also teaches away from the present invention. Kunzelman is directed towards a system for migrating a client-server session which **requires communication** between the server and the client. In order to migrate a session, a server node communicates “*a session token to the client*” (Kunzelman, col. 4, lines 33-34, FIG. 2, S3, 104). The client then “*sends [the] session token to the target server node*” (Kunzelman, col. 5, lines 38-40, FIG. 2, S4, 104). In other words, the invention of Kunzelman requires a server node to communicate with the client to migrate the session to another server node.

In contrast, the present invention is specifically directed towards a system for sharing (or migrating) a secure communication session which **does not require communication** between the server and the client. In order to share (or migrate) a session, a first server retrieves “*security state information from a second server, which has an active secure communication session with the client*” (page 4, lines 5-6). The first server then “*uses this state information to establish the active secure communication session with the client without having to communicate with the client*” (page 4, lines 7-9). To summarize, Kunzelman teaches away from the present invention, because, in contrast to Kunzelman, the present invention migrates (or shares) a secure communication session between server nodes without requiring communication between the server nodes and the client.

Additionally, the present invention has advantages over the inventions of Devarakonda and Kunzelman. The invention of Devarakonda requires a special node called a “*TCP router [whose] address is given out to clients, and client requests are sent thereto*” (Devarakonda, Abstract). This can increase the cost of the overall system due to the additional configuration and maintenance requirements for the TCP router. In contrast, the present invention does not require any special nodes, which can lead to substantial capital and operational cost savings (page 3, line 25 through page 5, line 21).

The invention of Kunzelman requires communication between the server and the client while migrating a session from one server to another (Kunzelman, col. 4, lines 33-34, col. 5, lines 38-40, FIG. 2, S3, S4, 104). This can add unnecessary delays to the migration operation. In contrast, the present invention does not add unnecessary delays to the migration operation because it does not require communication between the server and the client (page 4, lines 7-9).

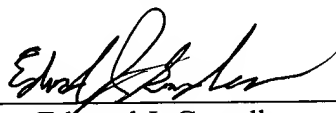
Accordingly, Applicant has amended independent claims 1, 13, and 25 to clarify that (1) the first server is different from the second server (note that this is in stark contrast to Devarakonda in which the SSL connection request is always routed to the same server node), and (2) the state information is purged from the second server after the state information is retrieved by the first server. These amendments find support on page 3, lines 25-26, page 4, lines 5-9, page 14, lines 8-10, FIG. 5, and FIG. 6 of the instant application.

Hence, Applicant respectfully submits that independent claims 1, 13, and 25 as presently amended are in condition for allowance. Applicant also submits that claims 2-10, which depend upon claim 1, claims 14-22, which depend upon claim 13, and claims 26-33, which depend upon claim 25, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

By 
Edward J. Grundler
Reg. No. 47,615

Date: 6 March 2006

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
2820 Fifth Street
Davis, CA 95616-7759
Tel: (530) 759-1663
FAX: (530) 759-1665
edward@parklegal.com